What is claimed is:

1. A method for facilitating reduction of a security threat in connection with transmission of an IP datagram having an IP header and an identification field in the IP header comprising:

supplementing the identification field of the IP header with at least one bit from another field of the IP header, whereby probability of random collisions is reduced, thereby reducing the security threat in connection with the transmission of the IP datagram.

2. A method for formatting an IP datagram having an IP header containing an identification field comprising:

a. determining identification information having a length greater than 16 bits associated with data to be sent in the IP datagram;

b. inserting at least one bit of the identification information into the identification field of the header; and

c. inserting remaining bits of the identification information into at least one other field of the header.

3. The method of claim 2 further comprising transmitting the IP datagram.

4. The method of claim 2 wherein the step of inserting the remaining bits of the identification information is carried out by inserting at least one of the remaining bits into a sub-network sub-field of at least one of a source address field and a destination address field of the header.

5. The method of claim 4 further comprising:

d. inserting source address information for the IP datagram into the source address field of the header;

e. inserting destination address information for the IP datagram into the destination address field of the header; and

f. inserting protocol information for the IP datagram into a protocol field of the header.

6. The method of claim 2 wherein the step of inserting the remaining bits of the identification information is carried out by inserting at least one of the remaining bits into a protocol field of the header.

7. The method of claim 6 additionally comprising:

d. inserting source address information for the IP datagram into the source address field of the header for the IP datagram;

e. inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and

f. inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram.

8. The method of claim 2 wherein the step of inserting the remaining bits of the identification information is carried out by inserting at least one of the remaining bits into a fragment offset field of the header.

9. The method of claim 8 further comprising:

d. inserting source address information for the IP datagram into a source address field of the header;

e. inserting destination address information for the IP datagram into a destination address field of the header; and

f. inserting protocol information for the IP datagram into a protocol field of the header.

10. The method of claim 2 wherein the step of inserting at least one bit is carried out by inserting 16 bits of the identification information into an identification field of the header

11. A method for formatting an IP datagram having an IP header comprising:

a. determining a special value based on a secret shared with a destination node; and

b. inserting at least a part of the special value into identification information carried by the header for the IP datagram, wherein a first portion of the identification information is included in the an identification field of the header and a second portion of the identification information is included in at least one other field of the header.

12. The method of claim 11 further comprising transmitting the IP datagram.

13. The method of claim 11 wherein in the determining step the special value is additionally based on at least one element selected from the group consisting of source address information, destination address information and at least one bit from the identification field.

14. The method of claim 11 wherein the inserting step is carried out by placing the part of the special value into the identification field.

15. The method of claim 14 further comprising:

c. inserting at least another part of the special value into the at least one other field of the header for.

16. The method of claim 14 wherein the part of the special value inserted into the identification field has a bit length less than 16 bits and the method further comprises:

c. determining additional identification information associated with the header for the IP datagram; and

d. inserting at least part of the additional identification information into the identification field of the header for the IP datagram.

17. The method of claim 16 further comprising:

e. inserting at least another part of the additional identification information into a field of the header for the IP datagram other than the identification field.

18. A method for facilitating fragmentation-free transmissions between two IPsec nodes implementing IPsec protocol, the method comprising:

a. transmitting a plurality of packets of differing size from a first IPsec node to a second IPsec node, each packet having an IP header wherein a "Don't Fragment" (DF) bit in a fragmentation flag field in the header for each packet of the plurality is set to a value that is arranged to prevent fragmentation of the packet en route; and

b. determining a maximum packet size for avoiding fragmentation in transmissions from the first IPsec node to the second IPsec node based on at least one response from the second IPsec node to the plurality of packets transmitted by the first IPsec node.

19. The method of claim 18 further comprising:

c. transmitting at least one packet from the first IPsec node to the second IPsec node, wherein the packet size of the at least one packet is less than or equal to the maximum packet size.

20. A method for assembling a plurality of received IP datagrams each having an IP header comprising:

assembling the plurality of received IP datagrams based on identification information contained in an identification field and at least one other field of the header for each of the received IP datagrams, wherein the identification information for each received IP datagram does not include source address information, destination address information or protocol information for that received IP datagram.

21. The method of claim 20 wherein the at least one other field comprises at least one field selected from the group consisting of the sub-net subfield of at least one of the source address field and the destination address field of the header for each received IP datagram, the protocol

field of the header for each received IP datagram and the fragment offset field of the header for each received IP datagram.

22. A method for assembling IP datagrams each having an IP header, the method comprising:

a. receiving a plurality of the IP datagrams;

b. extracting identification information from each of the plurality of the IP datagrams, the identification information for each of the IP datagrams comprising 16 bits of an identification field and at least one bit from at least one other field of the header for that IP datagram, the at least one bit not including source address information, destination address information or protocol information for the IP datagram;

c. identifying a subset of the plurality of the IP datagrams based on the identification information and at least one element selected from the group consisting of the source address information, the destination address information and the protocol information for each IP datagram from the subset; and

d. assembling the subset of the plurality of the IP datagrams into a message based on fragmentation offset information from a fragmentation offset field of the header for each IP datagram from the subset.

23. The method of claim 22 wherein the at least one other field of the header for that IP datagram is selected from the group consisting of the sub-net subfield of at least one of the source address field and the destination address field of the header for that IP datagram, the protocol field of the header for that IP datagram and the fragmentation offset field of the header for that IP datagram.

24. The method of claim 22 wherein the identifying step comprises:

e. determining a special value based on a secret shared with a source node; and

f. identifying at least one IP datagram from the plurality as part of the subset based on the at least one IP datagram's containing the special value as part of the identification information for the at least one IP datagram.

25. The method of claim 24 wherein in the determining step the special value is additionally based on at least one element selected from the group consisting of the source address information, the destination address information and at least one bit from the identification field of the header for the at least one IP datagram.

26. A method for facilitating fragmentation-free transmissions between two IPsec nodes implementing IPsec protocol, the method comprising:

a. receiving a plurality of packets of differing size from a first one of the IPsec nodes at a second one of the IPsec nodes, each of the packets having an IP header; wherein a "Don't Fragment" (DF) bit in a fragmentation flag field in the header for each packet is set to a value that is arranged to prevent fragmentation of the packet en route;

b. determining a maximum packet size for avoiding fragmentation in transmissions from a first security gateway to a second security gateway based on the received plurality of packets; and

c. transmitting a feedback message to the first IPsec node from the second IPsec node with an indication of the maximum packet size.

27. The method of claim 26 further comprising:

d. receiving at least one packet from the first IPsec node at the second IPsec node after the transmitting step wherein the at least one packet has a packet size less than or equal to the maximum packet size.

28. An apparatus for facilitating reduction of a security threat in connection with transmission of an IP datagram having an IP header and an identification field in the IP header comprising:

means for supplementing the identification field with at least one bit from another field of the IP header, whereby the security threat in connection with the transmission of the IP datagram is reduced.

29. An apparatus for formatting an IP datagram having an IP header comprising:

means for determining identification information having a length greater than 16 bits associated with data to be sent in the IP datagram;

means for inserting at least one bit of the identification information into an identification field of the header for the IP datagram; and

means for inserting remaining bits of the identification information into at least one field of the header of the IP datagram other than the identification field.

30. The apparatus of claim 29 further comprising means for transmitting the IP datagram.

31. The apparatus of claim 29 wherein the means for inserting the remaining bits of the identification information insert at least one of the remaining bits into the sub-network sub-field of at least one of the source address field and the destination address field of the header for the IP datagram.

32. The apparatus of claim 31 further comprising:

means for inserting source address information for the IP datagram into the source address field of the header for the IP datagram;

means for inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and

means for inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram.

33. The apparatus of claim 29 wherein the means for inserting the remaining bits of the identification information insert at least one of the remaining bits into the protocol field of the header for the IP datagram.

34. The apparatus of claim 33 additionally comprising:

means for inserting source address information for the IP datagram into the source address field of the header for the IP datagram;

means for inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and

means for inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram.

35. The apparatus of claim 29 wherein the means for inserting the remaining bits of the identification information insert at least one of the remaining bits into the fragment offset field of the header for the IP datagram.

36. The apparatus of claim 35 further comprising:

means for inserting source address information for the IP datagram into the source address field of the header for the IP datagram;

means for inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and

means for inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram.

37. The apparatus of claim 29 wherein the means for inserting at least one bit insert 16 bits of the identification information into the identification field of the header for the IP datagram.

38. An apparatus for formatting an IP datagram having an IP header comprising:

means for determining a special value based on a secret shared with a destination node; and

means for inserting at least a part of the special value into identification information carried by the header for the IP datagram, wherein a first portion of the identification information is included in an identification field and a second portion of the identification information is included in at least one other field of the header of the IP datagram.

39. The apparatus of claim 38 further comprising means for transmitting the IP datagram.

40. The apparatus of claim 38 wherein the means for determining the special value bases the determination on at least one element selected from the group consisting of source address information, destination address information and at least one bit from the identification field of the header for the IP datagram.

41. The apparatus of claim 38 wherein the means for inserting inserts the part of the special value into the identification field of the header for the IP datagram.

42. The apparatus of claim 41 further comprising:

means for inserting at least another part of the special value into the at least one other field of the header for the IP datagram.

43. The apparatus of claim 41 wherein the part of the special value inserted into the identification field has a bit length less than 16 bits and the apparatus further comprises:

means for determining additional identification information associated with the header for the IP datagram; and

means for inserting at least part of the additional identification information into the identification field of the header for the IP datagram.

44. The apparatus of claim 43 further comprising:

means for inserting at least another part of the additional identification information into a field of the header for the IP datagram other than the identification field.

45. An apparatus for facilitating fragmentation-free transmissions between two IPsec nodes implementing IPsec protocol, the apparatus comprising:

means for transmitting a plurality of packets of differing size from a first one of the IPsec nodes to a second one of the IPsec nodes, each of the packets having an IP header, wherein a "Don't Fragment" (DF) bit in a fragmentation flag field in the header

for each packet of the plurality is set to a value that is arranged to prevent fragmentation of the packet en route; and

means for determining a maximum packet size for avoiding fragmentation in transmissions from the first IPsec node to the second IPsec node based on at least one response from the second IPsec node to the plurality of packets transmitted by the first IPsec node.

46. The apparatus of claim 45 further comprising:

means for transmitting at least one packet from the first IPsec node to the second IPsec node, wherein the packet size of the at least one packet is less than or equal to the maximum packet size.

47. An apparatus for assembling a plurality of received IP datagrams each having an IP header comprising:

means for assembling the plurality of received IP datagrams based on identification information contained in an identification field of the header for each received IP datagram and at least one other field of the header for each received IP datagram, wherein the identification information for each one of the received IP datagrams does not include source address information, destination address information or protocol information for that received IP datagram.

48. The apparatus of claim 47 wherein the at least one other field comprises at least one field selected from the group consisting of the sub-net subfield of at least one of the source address field and the destination address field of the header for each received IP datagram, the protocol field of the header for each received IP datagram and the fragment offset field of the header for each received IP datagram.

49. An apparatus for assembling IP datagrams each having an IP header comprising:

means for receiving a plurality of IP datagrams;

means for extracting identification information from each of the plurality of IP datagrams, the identification information for each IP datagram comprising 16 bits of an

identification field of the header for that IP datagram and at least one bit from at least one other field of the header for that IP datagram, the at least one bit not including source address information, destination address information or protocol information for the IP datagram;

means for identifying a subset of the plurality of IP datagrams based on the identification information and at least one element selected from the group consisting of the source address information, the destination address information and the protocol information for each IP datagram from the subset; and

means for assembling the subset of the plurality of IP datagrams into a message based on fragmentation offset information from a fragmentation offset field of the header for each IP datagram from the subset.

50. The apparatus of claim 49 wherein the at least one other field of the header for that IP datagram is selected from the group consisting of the sub-net subfield of at least one of the source address field and the destination address field of the header for that IP datagram, the protocol field of the header for that IP datagram, the protocol field of the header for that IP datagram and the fragmentation offset field of the header for that IP datagram.

51. The apparatus of claim 49 wherein the means for identifying further comprises:

means for determining a special value based on a secret shared with a source node; and

means for identifying at least one IP datagram from the plurality as part of the subset based on the at least one IP datagram's containing the special value as part of the identification information for the at least one IP datagram.

52. The apparatus of claim 51 wherein the means for determining additionally bases the determination on at least one element selected from the group consisting of the source address information, the destination address information and at least one bit from the identification field of the header for the at least one IP datagram.

53. An apparatus for facilitating fragmentation-free transmissions between two IPsec nodes implementing IPsec protocol, the apparatus comprising:

means for receiving a plurality of packets of differing size from a first one of the IPsec nodes at a second one of the IPsec nodes, each of the packets having an IP header, wherein a "Don't Fragment" (DF) bit in a fragmentation flag field in the header for each packet from the plurality of packets is set to a value preventing fragmentation of the packet en route;

means for determining a maximum packet size for avoiding fragmentation in transmissions from a first security gateway to a second security gateway based on the received plurality of packets; and

means for transmitting a feedback message to the first IPsec node from the second IPsec node with an indication of the maximum packet size.

54. The apparatus of claim 54 further comprising:

means for receiving at least one packet from the first IPsec node at the second IPsec node after the transmitting step wherein the at least one packet has a packet size less than or equal to the maximum packet size.

55. A computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for facilitating reduction of security threats in connection with transmission of an IP datagram having an IP header and an identification field in the IP header, the method comprising:

supplementing the identification field of the IP header of the IP datagram with at least one bit from another field of the IP header, whereby the security threats in connection with the transmission of the IP datagram are reduced.

56. A computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for formatting an IP datagram having an IP header comprising:

a. determining identification information having a length greater than 16 bits associated with data to be sent in the IP datagram;

b. inserting at least one bit of the identification information into an identification field of the header for the IP datagram; and

c. inserting the remaining bits of the identification information into at least one field of the header of the IP datagram other than the identification field.

57. The computer-readable medium of claim 56 wherein the method further comprises transmitting the IP datagram.

58. The computer-readable medium of claim 56 wherein the step of inserting the remaining bits of the identification information is carried out by inserting at least one of the remaining bits into the sub-network sub-field of at least one of the source address field and the destination address field of the header for the IP datagram.

59. The computer-readable medium of claim 58 wherein the method further comprises:

d. inserting source address information for the IP datagram into the source address field of the header for the IP datagram;

e. inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and

f. inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram.

60. The computer-readable medium of claim 56 wherein the step of inserting the remaining bits of the identification information is carried out by inserting at least one of the remaining bits into the protocol field of the header for the IP datagram.

61. The computer-readable medium of claim 60 wherein the method further comprises:

d. inserting source address information for the IP datagram into the source address field of the header for the IP datagram;

e. inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and

f. inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram.

62. The computer-readable medium of claim 56 wherein the step of inserting the remaining bits of the identification information is carried out by inserting at least one of the remaining bits into the fragment offset field of the header for the IP datagram.

63. The computer-readable medium of claim 62 wherein the method further comprises:

d. inserting source address information for the IP datagram into the source address field of the header for the IP datagram;

e. inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and

f. inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram.

64. The computer-readable medium of claim 56 wherein the step of inserting at least one bit is carried out by inserting 16 bits of the identification information into the identification field of the header for the IP datagram.

65. A computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for formatting an IP datagram having an IP header, the method comprising:

a. determining a special value based on a secret shared with a destination node; and

b. inserting at least a part of the special value into identification information carried by the header for the IP datagram, wherein a first portion of the identification information is included in an identification field and a second portion of the identification information is included in at least one other field of the header of the IP datagram.

66. The computer-readable medium of claim 65 wherein the method further comprises transmitting the IP datagram.

67. The computer-readable medium of claim 65 wherein in the determining step in the method the special value is additionally based on at least one element selected from the group consisting of source address information, destination address information and at least one bit from the identification field of the header for the IP datagram.

68. The computer-readable medium of claim 65 wherein the inserting step is carried out by placing the part of the special value into the identification field of the header for the IP datagram.

69. The computer-readable medium of claim 68 wherein the method further comprises:

c. inserting at least another part of the special value into the at least one other field of the header for the IP datagram.

70. The computer-readable medium of claim 68 wherein the at least part of the special value inserted into the identification field has a bit length less than 16 bits and the method further comprises:

c. determining additional identification information associated with the header for the IP datagram; and

d. inserting at least part of the additional identification information into the identification field of the header for the IP datagram.

71. The computer-readable medium of claim 70 wherein the method further comprises:

e. inserting at least another part of the additional identification information into a field of the header for the IP datagram other than the identification field.

72. A computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for facilitating fragmentation-free transmissions between two IPsec nodes implementing the IPsec protocol, the method comprising:

a. transmitting a plurality of packets of differing size from a first IPsec node to a second IPsec node, wherein the "Don't Fragment" (DF) bit in the fragmentation flag field in the header for each packet of the plurality is set to a value that is arranged to prevent fragmentation of the packet en route; and

b. determining a maximum packet size for avoiding fragmentation in transmissions from the first IPsec node to the second IPsec node based on at least one response from the second IPsec node to the plurality of packets transmitted by the first IPsec node.

73. The computer-readable medium of claim 72 wherein the method further comprises:

c. transmitting at least one packet from the first IPsec node to the second IPsec node, wherein the packet size of the at least one packet is less than or equal to the maximum packet size.

74. A computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for assembling a plurality of received IP datagrams, the method comprising:

assembling the plurality of received IP datagrams based on identification information contained in the identification field of the header for each received IP datagram and at least one other field of the header for each received IP datagram, wherein the identification information for each received IP datagram does not include source

address information, destination address information or protocol information for that received IP datagram.

75. The computer-readable medium of claim 74 wherein the at least one other field comprises at least one field selected from the group consisting of the sub-net subfield of at least one of the source address field and the destination address field of the header for each received IP datagram, the protocol field of the header for each received IP datagram and the fragment offset field of the header for each received IP datagram.

76. A computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for assembling IP datagrams, the method comprising:

a. receiving a plurality of IP datagrams;

b. extracting identification information from each of the plurality of IP datagrams, the identification information for each IP datagram comprising 16 bits of the identification field of the header for that IP datagram and at least one bit from at least one other field of the header for that IP datagram, the at least one bit not including source address information, destination address information or protocol information for the IP datagram;

c. identifying a subset of the plurality of IP datagrams based on the identification information and at least one element selected from the group consisting of the source address information, the destination address information and the protocol information for each IP datagram from the subset; and

d. assembling the subset of the plurality of IP datagrams into a message based on fragmentation offset information from the fragmentation offset field of the header for each IP datagram from the subset of the plurality of IP datagrams.

77. The computer-readable medium of claim 76 wherein the at least one other field of the header for that IP datagram is selected from the group consisting of the sub-net subfield of at least one of the source address field and the destination address field of the header for that IP

datagram, the protocol field of the header for that IP datagram and the fragmentation offset field of the header for that IP datagram.

78. The computer-readable medium of claim 76 wherein the identifying step in the method comprises:

e. determining a special value based on a secret shared with a source node; and

f. identifying at least one IP datagram from the plurality as part of the subset based on the at least one IP datagram's containing the special value as part of the identification information for the at least one IP datagram.

79. The computer-readable medium of claim 78 wherein in the determining step in the method the special value is additionally based on at least one element selected from the group consisting of the source address information, the destination address information and at least one bit from the identification field of the header for the at least one IP datagram.

80. A computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for facilitating fragmentation-free transmissions between two IPsec nodes implementing the IPsec protocol, the method comprising:

a. receiving a plurality of packets of differing size from a first IPsec node at a second IPsec node, wherein the "Don't Fragment" (DF) bit in the fragmentation flag field in the header for each packet from the plurality of packets is set to a value preventing fragmentation of the packet en route;

b. determining a maximum packet size for avoiding fragmentation in transmissions from the first security gateway to the second security gateway based on the received plurality of packets; and

c. transmitting a feedback message to the first IPsec node from the second IPsec node with an indication of the maximum packet size.

81. The computer-readable medium of claim 80 wherein the method further comprises:

receiving at least one packet from the first IPsec node at the second IPsec node after the transmitting step wherein the at least one packet has a packet size less than or equal to the maximum packet size.

82. A method for facilitating the reduction of a security threat in connection with the transmission of an IP datagram having an IP header and an identification field in the IP header comprising:

supplementing the identification field of the IP header of the IP datagram with at least one bit from another field of the IP header, wherein the remaining bits of the another field contain an amount of information that is sufficient for an intermediate node or a receiving node to carry out the functionality normally corresponding to the another field.

83. A signal, embedded in a medium, comprising:

data representing an IP packet wherein the identification field of the IP header of the IP packet is supplemented with at least one bit from another field of the IP header, wherein the remaining bits of the another field contain an amount of information that is sufficient for an intermediate node or a receiving node to carry out the functionality normally corresponding to the another field.

84. A computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for facilitating fragmentation-free transmissions between two IPsec nodes implementing the IPsec protocol, the method comprising:

supplementing the identification field of the IP header of the IP datagram with at least one bit from another field of the IP header, wherein the remaining bits of the another field contain an amount of information that is sufficient for an intermediate node or a receiving node to carry out the functionality normally corresponding to the another field.